(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **06162289 A**

(43) Date of publication of application: **10 . 06 . 94**

(51) Int. Cl **G06K 19/10**
G06F 15/21
G06K 17/00
G09C 1/00

(21) Application number: **04308688**

(22) Date of filing: **18 . 11 . 92**

(71) Applicant: **NIPPON TELEGR & TELEPH CORP <NTT>**

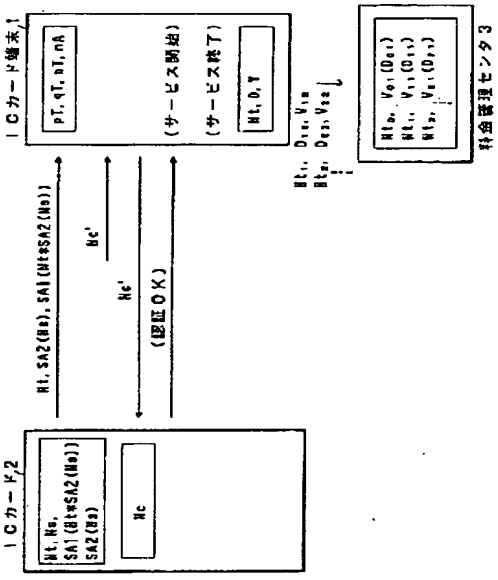
(72) Inventor: **ISHIGURO GINYA**
MUTA TOSHIYASU
SAKIDA KAZUTAKA

(54) **IC CREDIT CARD AND IC CARD TERMINAL**

(57) Abstract:

PURPOSE: To dispense with the check of the legality of an user by a center at the time of receiving service.

CONSTITUTION: At the time of issueing an IC card 2, a registration number Nt assigned at every user, a set number Ns for setting a password number use, a digital signature SA2 (Ns) prepared by the master key of an issuer and the digital signature SA1{Nt*SA1(Ns)} prepared by the master key with SA2 (Ns) and Nt are stored in the EEPROM of the IC card 2. At the time of registering the password number Nc, the legality of the user is checked and verified with the IC card 2 by communication with an IC card terminal 1 by Ns known only to the user. By inserting the IC card 2, Nt, SA2 and SA1 are transmitted to the terminal 1 and the terminal 1 verifies SA1 by an open key nA, checks the legality of Nt and when it is correct, let the password number be inputted. When the user inputs Nc', the IC card 2 compares it with Nc of the inside and transmits authentication to the terminal 1 in the case of coincidence and when it is received, the terminal 1 permits the user to receive the service.



(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号

特開平6－162289

(43)公開日　平成６年(1994)６月10日

(51)Int.Cl.[5]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０６Ｋ　19/10				
Ｇ０６Ｆ　15/21	３４０　Ｂ	7052－5Ｌ		
Ｇ０６Ｋ　17/00	Ｔ	7459－5Ｌ		
Ｇ０９Ｃ　1/00		8837－5Ｌ		
		8623－5Ｌ	Ｇ０６Ｋ　19/00　Ｒ	

審査請求　未請求　請求項の数２(全 10 頁)

(21)出願番号　特願平4－308688

(22)出願日　平成４年(1992)11月18日

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区内幸町一丁目１番６号

(72)発明者　石黒　銀矢
東京都千代田区内幸町１丁目１番６号　日本電信電話株式会社内

(72)発明者　牟田　敏保
東京都千代田区内幸町１丁目１番６号　日本電信電話株式会社内

(72)発明者　崎田　一貴
東京都千代田区内幸町１丁目１番６号　日本電信電話株式会社内

(74)代理人　弁理士　草野　卓

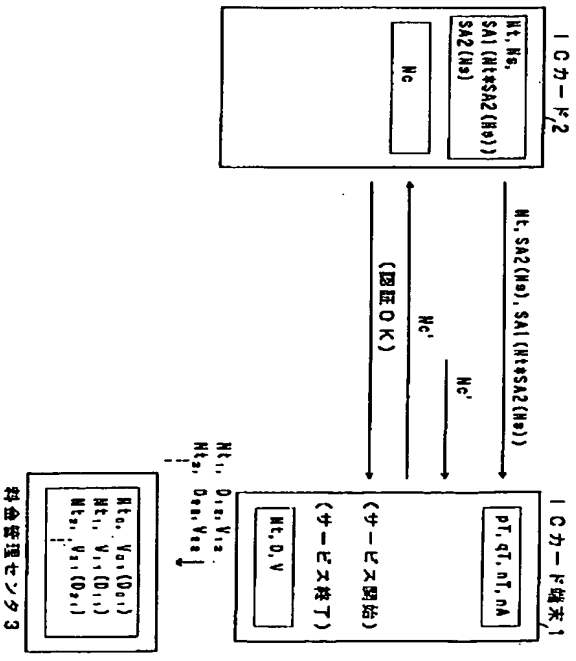
(54)【発明の名称】　ＩＣクレジットカード及びＩＣカード端末

(57)【要約】　(修正有)

【目的】　サービスを受けるに当りセンタによる利用者の正当性のチェックの不要化。

【構成】　ＩＣカード２発行の際、利用者ごとに割付けられた登録番号Ｎｔと、暗証番号設定用設定番号Ｎｓと、発行者のマスタ鍵でＮｓに作成したデジタル署名ＳＡ２（Ｎｓ）と、ＳＡ２（Ｎｓ）とＮｔにマスタ鍵で作成したデジタル署名ＳＡ１（Ｎｔ＊ＳＡ１（Ｎｓ））とをＩＣカード２のＥＥＰＲＯＭに記憶しておく。暗証番号Ｎｃ登録の際は、利用者しか知らないＮｓで利用者の正当性をＩＣカード端末１とのやりとりでＩＣカード２でチェック検証する。ＩＣカード２の挿入で、Ｎｔ、ＳＡ２、ＳＡ１が端末１へ送られ、端末１は公開鍵ｎＡでＳＡ１を検証し、Ｎｔの正当性をチェックし、正しければ暗証番号を入力させる。利用者のＮｃ′入力で、ＩＣカード２は内部のＮｃと比較し、一致すれば認証化を端末１へ送り端末１はこれを受けると利用者にサービスを受けることを許す。

図５



1

【特許請求の範囲】

【請求項１】　利用者を特定するための登録番号Ｎｔ、暗証番号を設定するための設定番号Ｎｓ、前記登録番号Ｎｔを含む情報に対するマスタ鍵によるデジタル署名ＳＡを記録するとともに、暗証番号Ｎｃを記録するためのメモリと、

前記登録番号Ｎｔ、前記デジタル署名ＳＡをＩＣカード端末へ送信する手段と、

前記ＩＣカード端末から受信した設定番号Ｎｓ′と前記メモリに記録している設定番号Ｎｓとの比較を行い、一致したとき第１の認証通知を前記ＩＣカード端末へ送信する手段と、

暗証番号登録時に、前記ＩＣカード端末から暗証番号Ｎｃ、その暗証番号Ｎｃを含む情報に対する前記ＩＣカード端末によるデジタル署名ＳＴ、前記ＩＣカード端末の端末公開鍵ｎＴを受信し、前記受信したデジタル署名ＳＴを受信した端末公開鍵ｎＴで検証し、正しい場合にのみ前記メモリに受信した暗証番号Ｎｃを記録する手段と、

サービス開始前に、前記ＩＣカード端末から受信した暗証番号Ｎｃ′と前記メモリに記録している暗証番号Ｎｃとの比較を行い、一致したとき第２の認証通知を前記ＩＣカード端末へ送信する手段と、

を具備するＩＣクレジットカード。

【請求項２】　デジタル署名ＳＡを検証するためのマスタ公開鍵ｎＡ及び端末公開鍵ｎＴ、デジタル署名をするための端末鍵ｐＴ、ｑＴを記録したメモリと、

ＩＣカードから受信したデジタル署名ＳＡを前記公開鍵ｎＡで検証し、受信した登録番号Ｎｔが正しければ暗証番号の登録または暗証番号の入力を許可する手段と、

暗証番号の登録が選択されたとき、入力手段から入力された登録番号Ｎｔ′と受信した登録番号Ｎｔとの比較を行い、一致したとき設定番号の入力を指示する手段と、

前記入力手段から入力された設定番号Ｎｓ′を前記ＩＣカードへ送信する手段と、

前記ＩＣカードから第１の認証通知を受信したとき、前記入力手段から入力された暗証番号Ｎｃを含む情報に対して前記端末鍵ｐＴ、ｑＴを用いてデジタル署名ＳＴを作成する手段と、

前記暗証番号Ｎｃ、前記デジタル署名ＳＴ、前記端末公開鍵ｎＴを前記ＩＣカードに送信する手段と、

暗証番号の入力が選択されたとき、前記入力手段から入力された暗証番号Ｎｃ′を前記ＩＣカードに送信する手段と、

前記ＩＣカードから第２の認証通知を受信したとき、サービスを許可する手段と、

を具備したＩＣカード端末。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】この発明は、あらかじめ登録番号

2

などを登録してあるＩＣカードをＩＣカード端末へ利用者が挿入することによりサービスの提供を受け、そのサービスについて後に料金の請求を受けるようにしたＩＣクレジットカードシステムに用いられる前記ＩＣクレジットカード及び前記ＩＣカード端末に関する。

【０００２】

【従来の技術】従来のＩＣクレジットカードシステムは、サービス提供前に、ＩＣカード端末と、登録番号などを登録しているセンタとをオンラインでつなぎ、利用者がダイヤル操作により登録番号などを入力し、入力された情報がセンタに送られ、センタであらかじめ登録されている利用者情報により利用者の正当性のチェックが行われ、正当であることが確認されたとき、ＩＣカード端末でのサービスの提供を可能としていた。

【０００３】

【発明が解決しようとする課題】したがって、従来においては、サービス提供前にセンタとＩＣカード端末とが通信を行う必要があり、オンラインで検証を行うためにセンタ設備が大規模になったり、通信料がサービス提供料金の他に必要になるなど欠点があった。

【０００４】

【課題を解決するための手段】この発明によるＩＣクレジットカードは、利用者を特定するための登録番号Ｎｔ、暗証番号を設定するための設定番号Ｎｓ、前記登録番号Ｎｔを含む情報に対するマスタ鍵によるデジタル署名ＳＡを記録するとともに、暗証番号Ｎｃを記録するためのメモリと、前記登録番号Ｎｔ、前記デジタル署名ＳＡをＩＣカード端末へ送信する手段と、前記ＩＣカード端末から受信した設定番号Ｎｓ′と前記メモリに記録している設定番号Ｎｓとの比較を行い、一致したとき第１の認証通知を前記ＩＣカード端末へ送信する手段と、暗証番号登録時に、前記ＩＣカード端末から暗証番号Ｎｃ、前記暗証番号を含む情報に対する前記ＩＣカード端末によるデジタル署名ＳＴ、前記ＩＣカード端末の端末公開鍵ｎＴを受信し、その受信したデジタル署名ＳＴを前記端末公開鍵ｎＴで検証し、正しい場合にのみ前記メモリに受信した暗証番号Ｎｃを記録する手段と、サービス開始前に、前記ＩＣカード端末から受信した暗証番号Ｎｃ′と前記メモリに記録している暗証番号Ｎｃとの比較を行い、一致したとき第２の認証通知を前記ＩＣカード端末へ送信する手段とを具備する。

【０００５】この発明によるＩＣカード端末は、デジタル署名ＳＡを検証するためのマスタ公開鍵ｎＡ及び端末公開鍵ｎＴ、デジタル署名をするための端末鍵ｐＴ、ｑＴを記録したメモリと、受信したデジタル署名ＳＡを前記公開鍵ｎＡで検証し、受信した登録番号Ｎｔが正しければ暗証番号の登録または暗証番号の入力を許可する手段と、暗証番号の登録が選択されたとき、入力手段から入力された登録番号Ｎｔ′と受信した登録番号Ｎｔとの比較を行い、一致したとき設定番号の入力を指示する手

段と、入力手段から入力された設定番号Ｎｓ′をＩＣカードへ送信する手段と、前記ＩＣカードから第１の認証通知を受信したとき、入力手段から入力された暗証番号Ｎｃを含む情報に対して前記端末鍵ｐＴ、ｑＴを用いてデジタル署名ＳＴを作成する手段と、前記暗証番号Ｎｃ、前記デジタル署名ＳＴ、前記端末公開鍵ｎＴを前記ＩＣカードに送信する手段と、暗証番号の入力が選択されたとき、入力手段から入力された暗証番号Ｎｃ′を前記ＩＣカードに送信する手段と、前記ＩＣカードから第２の認証通知を受信したとき、サービスを許可する手段とを具備する。

【０００６】

【作用】このような構成のＩＣクレジットカード（以下単にＩＣカードと記す）、ＩＣカード端末を設ければ、デジタル署名付きの登録番号によってＩＣカードの正当性をＩＣカード端末で検証できるとともに、利用者が入力した暗証番号により、利用者の正当性をＩＣカードで検証でき、さらに暗証番号の登録時には利用者しか知り得ない設定番号により利用者の正当性をＩＣカードで検証できるので利用者の情報に関するデータベースを持つセンタへサービス開始前にアクセスする必要がなく、しかも不正なＩＣカードによるサービス利用も排除することができる。

【０００７】

【実施例】次に図を参照にして請求項１及び２の発明の各実施例を説明する。図１は、この発明のＩＣカード及びＩＣカード端末が適用されるＩＣクレジットカードシステム構成例を示す。ＩＣカード端末１はＩＣカード２により検証処理を行い、通話など各種サービスを提供する。料金管理センタ３はＩＣカード２により利用したサービス料金を管理する。ＩＣカード端末１は利用されたＩＣカード２の登録番号と利用料金をメモリに蓄えておき、適当な間隔、例えば日ごとに料金管理センタ３へ自動的に発信し、蓄えた情報を料金管理センタ３へ通信網４を介して送信する。料金管理センタ３では登録番号ごとに利用料金を集計し、例えば月ごとに利用者へ利用料金の請求を行う。

【０００８】図２はＩＣカード端末１の内部構成を示す図であり、制御部１１は処理手順などのプログラムを内部のＲＯＭに記録しているとともに、鍵情報などを内部ＲＡＭに記録している。鍵情報などは、ＩＣカード端末設置時に、通信網を介してセンタ装置（図示せず）と接続し、センタ装置から受信してＲＡＭに記録してもよく、ＩＣカード端末製造時に予め設定してもよい。ＩＣカード２とデータのやりとりを行うＩＣカードリーダライタ部１２、暗証番号の登録を指示する操作ボタン、ダイヤルボタンなどからなる操作入力部１３、液晶ディスプレイからなる表示部１４及び通話回路１５が制御部１１に接続され、通話回路１５に送受器１６が接続されまた通信網との処理を行う通信処理部１７が制御部１１に接続されている。

【０００９】図３はＩＣカード２の内部構成を示す図であり、ＩＣカードの処理手順等のプログラムはＲＯＭ６１に記憶され、ＣＰＵ６３はワークエリアとしてＲＡＭ６２を利用してすべての制御を行い、図２に示したＩＣカード端末１のＩＣカードリーダライタ部１２との通信は通信部６５により接点６６を介して行われる。登録番号、設定番号、デジタル署名はＩＣカード２の発行時にＩＣカード発行機（図示せず）によって書き込まれＥＥＰＲＯＭ６４に記録されている。

【００１０】図４は利用者がＩＣカード端末１を使ってＩＣカード２に暗証番号を登録する操作を説明する図である。ＩＣカード２のＥＥＰＲＯＭ６４の所定エリアに、利用者を特定するための登録番号Ｎｔ、暗証番号を設定するために利用者ごとに割り付けられた設定番号Ｎｓ、その設定番号Ｎｓに対して発行者がマスタ鍵によって作成した第２のデジタル署名ＳＡ２（Ｎｓ）、登録番号Ｎｔおよび第２のデジタル署名ＳＡ２（Ｎｓ）に対して発行者がマスタ鍵によって作成した第１のデジタル署名ＳＡ１（Ｎｔ＊ＳＡ２（Ｎｓ））が記録されている。この記録の際に第２のデジタル署名ＳＡ２（Ｎｓ）を公開鍵ｎＡで検証して設定番号Ｎｓの正当性を判断することができる。また、ＩＣカード端末１の制御部１１内のＲＡＭの所定のエリアに、前記マスタ鍵によって作成されたデジタル署名を検証するためのマスタ公開鍵ｎＡ、ＩＣカードが端末がデジタル署名を作成するための端末鍵ｐＴ、ｑＴ、前記ＩＣカード端末が作成したデジタル署名を検証するための端末公開鍵ｎＴが記録されている。デジタル署名としては、例えば「ＮＴＴ　Ｒ＆ＤＶｏｌ.40　No.5　P. 687～696（1991）」に掲載されているＥＳＩＧＮを使用することができる。

【００１１】利用者がＩＣカード２をＩＣカード端末１のＩＣカードリーダライタ部１２に挿入すると、ＩＣカード２からＩＣカード端末１に登録番号Ｎｔ、第２のデジタル署名ＳＡ２（Ｎｓ）、第１のデジタル番号ＳＡ１（Ｎｔ＊ＳＡ２（Ｎｓ））が送信される。ＩＣカード端末１はマスタ公開鍵ｎＡにより第１のデジタル署名ＳＡ１の検証を行い、Ｎｔの正当性を判断する。この場合第２のデジタル署名ＳＡ２の検証も行い、これの正当性も判断すると一そう正確になる。正当でないと判断した場合にはＩＣカードを返却して処理を中止する。両者とも正当であると判断した場合には“暗証番号の入力”を指示する画面を表示部１４に表示する。この画面が表示されている間は、暗証番号の入力を可能とするとともに、操作入力部１３のボタン操作による暗証番号の登録を有効とする。ここで、暗証番号を入力してもＩＣカード２に暗証番号が登録されていなければ暗証番号不一致として処理される。操作入力部１３の暗証番号登録ボタンを押すことにより暗証番号登録処理に移行する。ＩＣカード２へ暗証番号登録通知を送信し、ＩＣカード２へ暗証

番号登録処理に入ったことを知らせるとともに、表示部１４に“登録番号をダイヤルしてください”と表示し、利用者に登録番号の入力を促す。利用者がダイヤルにより登録番号Ｎｔ′を入力すると、ＩＣカード端末１は先にＩＣカード２から受信した登録番号Ｎｔとの比較を行い、利用者が入力した番号の正当性をチェックする。一致しない場合には再度登録番号の入力を促すが、例えば３回の入力後も一致しない場合には、不正使用と判断しＩＣカード２を返却して処理を中止する。一致した場合には表示部１４に“設定番号をダイヤルしてください”と表示し、利用者に設定番号の入力を促す。

【００１２】利用者がダイヤルにより設定番号Ｎｓ′を入力すると、ＩＣカード端末１はＩＣカード２へ設定番号Ｎｓ′を送信する。ＩＣカード２は受信した設定番号Ｎｓ′と前記メモリに予め記録している設定番号Ｎｓとの比較を行い、利用者が入力した設定番号の正当性をチェックする。一致しない場合にはＩＣカード端末１へ不一致通知を送信し、ＩＣカード端末１は再度設定番号の入力を促すが、例えば３回の入力後も一致しない場合には、不正使用と判断しＩＣカード２を返却して処理を中止する。一致した場合にはＩＣカード２は認証ＯＫ（第１の認証通知）をＩＣカード端末１へ送信する。ＩＣカード端末１は表示部１４に“暗証番号をダイヤルしてください”と表示し、利用者に暗証番号の入力を促す。利用者がダイヤルにより暗証番号Ｎｃを入力すると、ＩＣカード端末１は暗証番号Ｎｃに対して端末鍵ｐＴ、ｑＴによるデジタル署名ＳＴ（Ｎｃ）を作成し、ＩＣカード２に暗証番号Ｎｃとともにデジタル署名ＳＴ（Ｎｃ）および端末公開鍵ｎＴを送信する。ＩＣカード２は端末公開鍵ｎＴによりデジタル署名ＳＴ（Ｎｃ）の検証を行い、暗証番号Ｎｃの正当性のチェックを行う。正当であることが検証できた場合には暗証番号ＮｃをＲＡＭ６２に記録する。

【００１３】上記の処理において、設定番号Ｎｓの検証をＩＣカード２で行うようにしているが、最初に登録番号ＮｔをＩＣカード端末１へ送信するときに設定番号Ｎｓもいっしょに送信しておけばＩＣカード端末１で設定番号のチェックを行うことができる。ただし、この場合には設定番号Ｎｓという他人には知られてはならない情報がＩＣカード２から送信されるためセキュリティという面からは好ましくない。また、登録番号あるいは設定番号のダイヤル時に、３回の入力後も一致しない場合には、不正カードである旨をＩＣカード２に記録することにより、以降そのＩＣカードの使用を不能とすることもできる。

【００１４】図５は利用者がＩＣカード２を使ってＩＣカード端末１からサービスを受けるときの処理を説明する図である。ＩＣカード２のＲＡＭ６２には暗証番号Ｎｃが記録されている。利用者がＩＣカード２をＩＣカード端末１のＩＣカードリーダライタ部１２に挿入すると、ＩＣカード２からＩＣカード端末１に登録番号Ｎｔ、第２のデジタル署名ＳＡ２（Ｎｓ）、第１のデジタル署名ＳＡ１（Ｎｔ＊ＳＡ２（Ｎｓ））が送信される。ＩＣカード端末１はマスタ公開鍵ｎＡによりデジタル署名ＳＡ１の検証を行い、登録番号Ｎｔの正当性を判断する。この場合も第２のデジタル署名の正当性を判断した方がよい。正当でないと判断した場合にはＩＣカード２を返却し処理を中止する。正当であると判断した場合には“暗証番号の入力”を指示する画面を表示部１４に表示する。この画面が表示されている間は、暗証番号の入力を可能とするとともに、操作入力部１３のボタン操作による暗証番号の再登録も有効である。つまり暗証番号を変更することもできる。ここで、利用者が暗証番号Ｎｃ′をダイヤルすると、このＮｃ′はＩＣカード２へ送信され、ＩＣカード２内でその内部に記録してある暗証番号Ｎｃとの比較が行われる。一致しない場合にはＩＣカード２からＩＣカード端末１へ認証不一致通知が送信され、ＩＣカード端末１は再度暗証番号の入力を促す。例えば３回の入力後も一致しない場合には、不正使用と判断してＩＣカード２を返却して処理を中止する。

【００１５】一致した場合にはＩＣカード２は認証ＯＫ（第２の認証通知）をＩＣカード端末１へ送信する。ＩＣカード端末１は、所定のサービスが可能であることを表示部１４に表示し、所定のサービスを実行する。例えば通常の通話サービスであれば、相手の番号がダイヤルできる旨を表示し、利用者のダイヤルした相手に接続する。これにより通話サービスを受けることができ、利用者がそのサービス利用を終了すると、ＩＣカード端末１はその利用者を特定する登録番号Ｎｔ、利用日時Ｄ、利用料金Ｖを内部のメモリに記録し、ＩＣカード２を排出して処理を終了する。その内部のメモリに蓄えたデータは、例えば１日に一回程度の割合で料金管理センタ３に送信する。料金管理センタ３ではこれを受信して登録番号ごとに料金を集計し、毎月利用者に請求書を送付して料金の支払いを受ける。

【００１６】図６はこの発明の他の実施例を示し、利用者がＩＣカード端末１を使ってＩＣカード２に暗証番号を登録する操作を説明する図である。ＩＣカード２のＥＥＰＲＯＭ６４にはＮｔ、Ｎｓ、ＳＡ２（Ｎｓ）、ＳＡ１（Ｎｔ＊ＳＡ２（Ｎｓ））が記録されている他に、ＩＣカード２がデジタル署名を作成するためのカード鍵ｐＵおよびｑＵ、ＩＣカードが作成したデジタル署名を検証するためのカード公開鍵ｎＵも記録されている。また、ＩＣカード２およびＩＣカード端末１は各々乱数生成用のプログラムをメモリに記録している。暗証番号の登録処理において、前述した手順により登録番号、設定番号の検証を終え、利用者がダイヤルボタンから暗証番号Ｎｃを入力すると、ＩＣカード端末１は乱数Ｒを生成し、ＩＣカード２へ乱数Ｒを送信する。ＩＣカード２は乱数Ｘを生成し、受信した乱数Ｒおよび生成した乱数Ｘ

に対してカード鍵ｐＵ、ｑＵを用いてデジタル署名ＳＵ（Ｒ＊Ｘ）を作成し、作成したデジタル署名ＳＵ（Ｒ＊Ｘ）とともに乱数ＸおよびカードＵ開鍵ｎＵをＩＣカード端末１へ送信する。

【００１７】ＩＣカード端末１は受信したカード公開鍵ｎＵにより受信したデジタル署名ＳＵを検証し、ＩＣカード２が正当な相手であることを認証する。正当な相手であることを認証すると、乱数ＲおよびＸ、暗証番号Ｎｃに対して端末鍵ｐＴ、ｑＴによりデジタル署名ＳＴ（Ｒ＊Ｘ＊Ｎｃ）を作成し、作成したデジタル署名ＳＴ（Ｒ＊Ｘ＊Ｎｃ）とともに端末公開鍵ｎＴ、暗証番号ＮｃをＩＣカード２へ送信する。ＩＣカード２は受信した端末公開鍵ｎＴによりデジタル署名ＳＴを検証し、ＩＣカード端末１が正当な相手であることを認証するとともに暗証番号の正当性を認証し、暗証番号ＮｃをＲＡＭ６２に記録する。この実施例の場合には情報の送受に相互に生成した乱数を使用しているため信号の内容が同一になることがなく、傍受した信号を利用した不正を防止することができる。また、相互にデジタル署名を作成して相互認証を行っているためセキュリティをより高めることができる。

【００１８】図７はこの発明の他の実施例を示し、図６で説明したＩＣカード２およびＩＣカード端末１によりサービスを受けるときの処理を説明する図である。利用者がＩＣカード２をＩＣカード端末１へ挿入し、図５で前述した手順により登録番号の検証を終え、利用者がダイヤルボタンから暗証番号Ｎｃ′を入力すると、ＩＣカード端末１は乱数Ｒを生成し、ＩＣカード２へ乱数Ｒ、及び暗証番号Ｎｃ′を送信する。ＩＣカード２は受信した暗証番号Ｎｃ′とメモリに記録している暗証番号Ｎｃとの比較を行い、一致していれば乱数Ｘを生成し、受信した乱数Ｒおよび生成した乱数Ｘに対してカード鍵ｐＵ、ｑＵによりデジタル署名ＳＵ（Ｒ＊Ｘ）を作成し、その作成したデジタル署名ＳＵ（Ｒ＊Ｘ）とともに乱数ＸおよびカードＵ開鍵ｎＵをＩＣカード端末１へ送信する。ＩＣカード端末１は受信したカード公開鍵ｎＵにより受信したデジタル署名ＳＵを検証し、ＩＣカード２が正当な相手であることを認証するとともに暗証番号が正当であると判断し、所定のサービスが可能であることを表示部１４に表示し、所定のサービスを実行する。サービスが終了すると、利用者を特定する登録番号Ｎｔ、利用日時Ｄ、利用料金Ｖを内部のメモリに記録し、ＩＣカード２を排出して処理を終了する。

【００１９】上記の説明において、ＩＣカード２を特定するカード番号ＩＤＵと、カード番号に対して発行者がマスタ鍵により作成したデジタル署名ＳＡ（ＩＤＵ）とをＩＣカード２の発行時にＥＥＰＲＯＭ６４に記録しておき、ＩＣカード２をＩＣカード端末１に挿入したとき、登録番号Ｎｔとともにカード番号ＩＤＵ、デジタル署名ＳＡ（ＩＤＵ）を送信し、マスタ公開鍵によってＳＡを検証することによりカード番号の正当性をチェックするように構成すれば、ＩＣカード２の紛失などに対処することができる。すなわち、ＩＣカード２を紛失したときに利用者が発行者に申告することにより、発行者はＩＣカード２のカード番号をダウンロードによりＩＣカード端末１にブラックリストとして登録する。ＩＣカード端末１はＩＣカード２が挿入されたときカード番号ＩＤＵとブラックリストとを比較する。一致するＩＣカードがあった場合にはそのＩＣカードの使用を制限することができる。

【００２０】また、ＩＣカード２のＥＥＰＲＯＭ６４に日付情報を記録しておき、ＩＣカード２をＩＣカード端末１に挿入したとき、登録番号とともに日付情報を送信し、ＩＣカード端末１に内蔵したカレンダと比較することによりＩＣカード２の使用可否を判断するように構成すれば有効期限付きのＩＣカード２とすることができる。

【００２１】さらに、ＩＣカード２およびＩＣカード端末１に送信情報の暗号化のためのアルゴリズムと暗号化および復号化のための共通の鍵をメモリに記録しておくことにより、相互の通信を暗号通信により行うことができ、よりセキュリティを高めることができる。

【００２２】

【発明の効果】この発明によるＩＣカードとＩＣカード端末とを用いられば、ＩＣカードとＩＣカード端末との間で相互の正当性を検証することになり、かつ利用者の正当性を、ＩＣカード端末を介してＩＣカードで検証するようになり、サービスの利用時あるいは暗証番号の設定時に利用者の情報に関するデータベースを持つセンタへアクセスする必要がなく、容易にシステムを構築することができる。また、センタへアクセスする必要がないため検証時間も短縮でき、操作性にすぐれたシステムとなる。さらに、発行者しか知り得ないマスタ鍵によるデジタル署名により登録番号の検証を行うように構成しているため、例え他人の登録番号を知り得てもデジタル署名を作成することはできず、また、拾ったＩＣカードでは暗証番号が分からず、登録番号、設定番号が不明なため暗証番号を変更することも不可能でありセキュリティの高いシステムを構築することができる。

【図面の簡単な説明】

【図１】この発明のＩＣカード、ＩＣカード端末を使用してＩＣクレジットカードシステムを構成した例を示すブロック図。

【図２】この発明によるＩＣカード端末の構成例を示すブロック図。

【図３】この発明によるＩＣカードの構成例を示すブロック図。

【図４】この発明によるＩＣカードとＩＣカード端末とを用いて、ＩＣカードに暗証番号を登録する場合の処理手順を示す図。

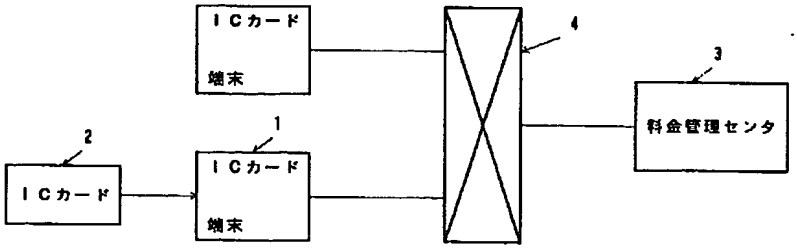
【図５】図４で示した手法で登録された暗証番号のＩＣカードによりサービスを受ける場合の処理手順を示す図。

【図６】この発明の他の実施例により暗証番号を登録する場合の処理手順を示す図。

【図７】図６で示した手順で登録された暗証番号のＩＣカードによりサービスを受ける場合の処理手順を示す図。

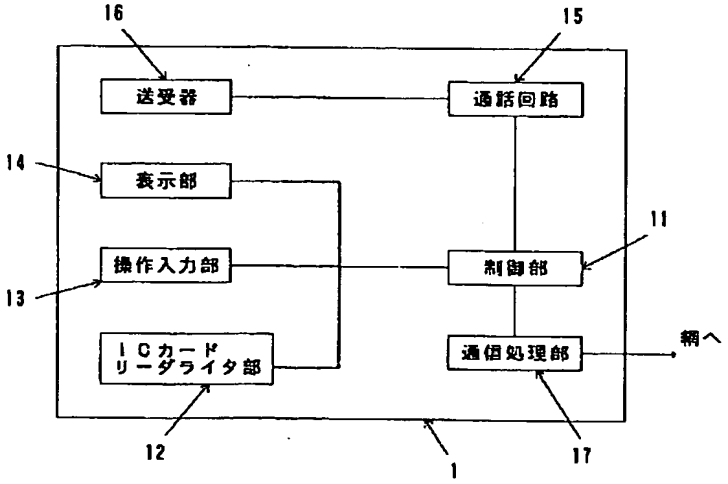
【図１】

図 1



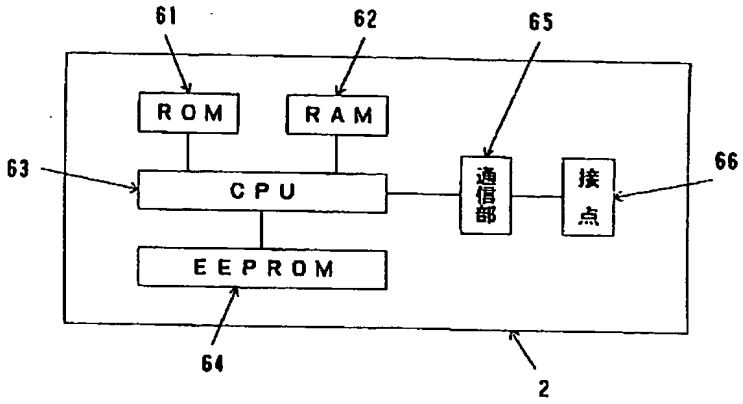
【図２】

図 2



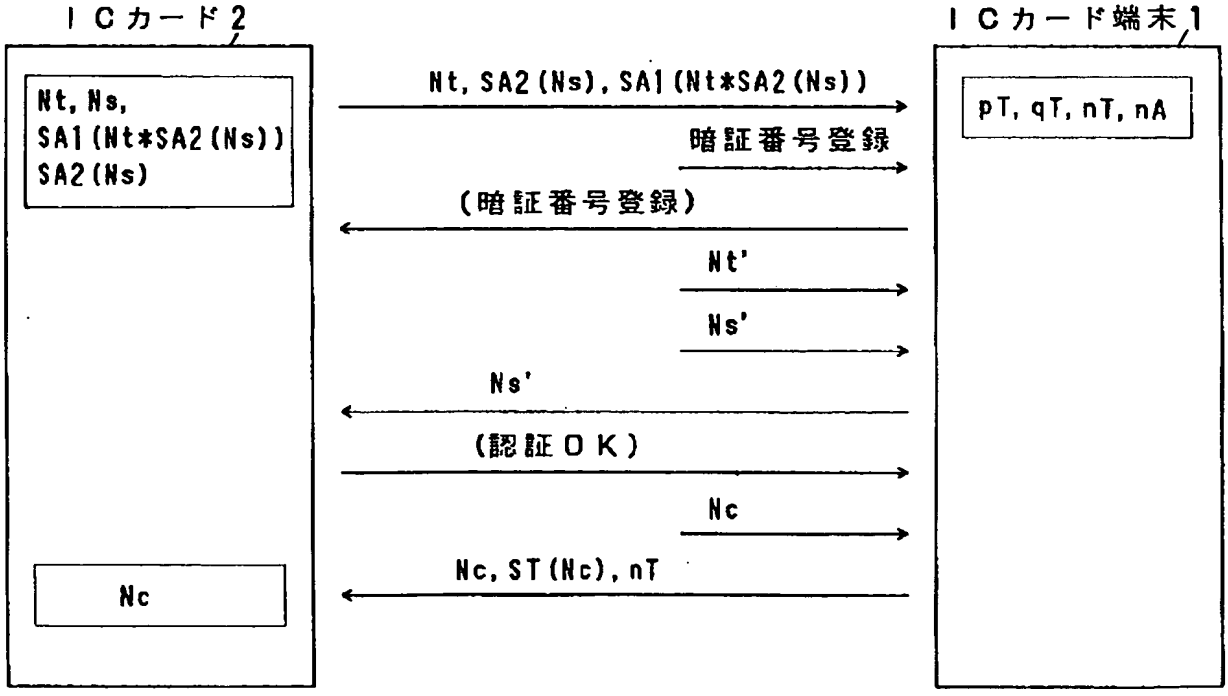
【図３】

図 3


61
62
65
ROM
RAM
63
CPU
通信部
接点
66
EEPROM
64
2

【図４】

図 4


ＩＣカード２
ＩＣカード端末１
Nt, Ns,
SA1(Nt*SA2(Ns))
SA2(Ns)
pT, qT, nT, nA
Nt, SA2(Ns), SA1(Nt*SA2(Ns))
暗証番号登録
(暗証番号登録)
Nt'
Ns'
Ns'
(認証ＯＫ)
Nc
Nc, ST(Nc), nT
Nc

【図5】

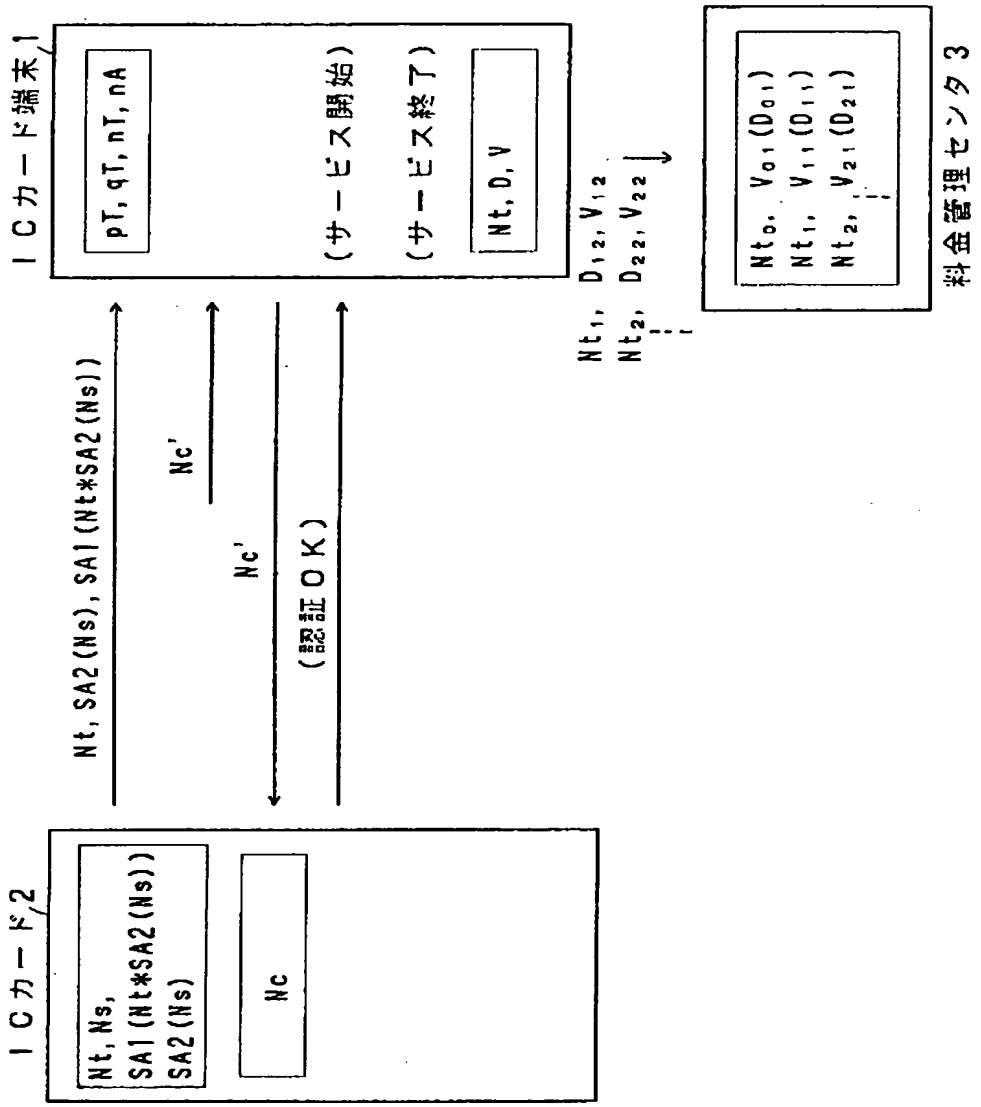
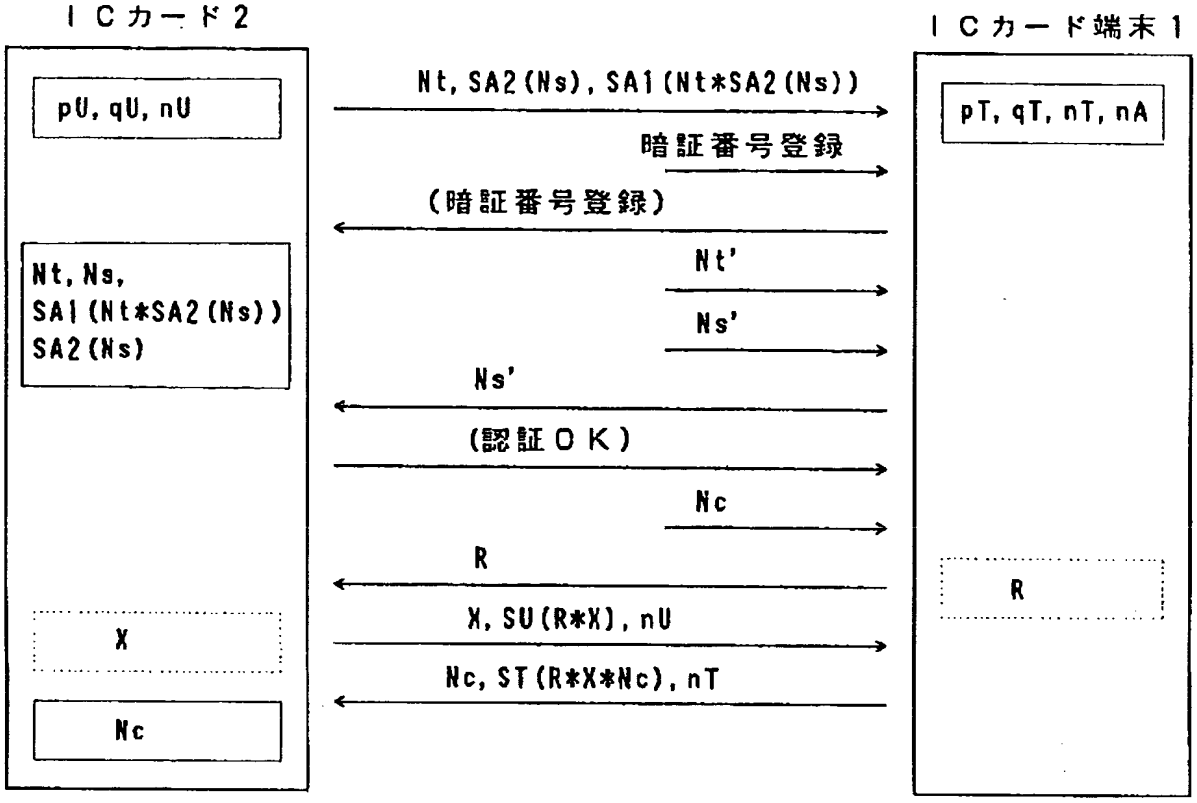

ICカード端末1
pT, qT, nT, nA
Nt, D, V
(サービス開始)
(サービス終了)
Nt, SA2(Ns), SA1(Nt*SA2(Ns))
Nc'
Nc'
(認証OK)
Nt1, D12, V12
Nt2, D22, V22
Nt0, V01(D01)
Nt1, V11(D11)
Nt2, V21(D21)
料金管理センタ3
ICカード2
Nt, Ns,
SA1(Nt*SA2(Ns))
SA2(Ns)
Nc

図5

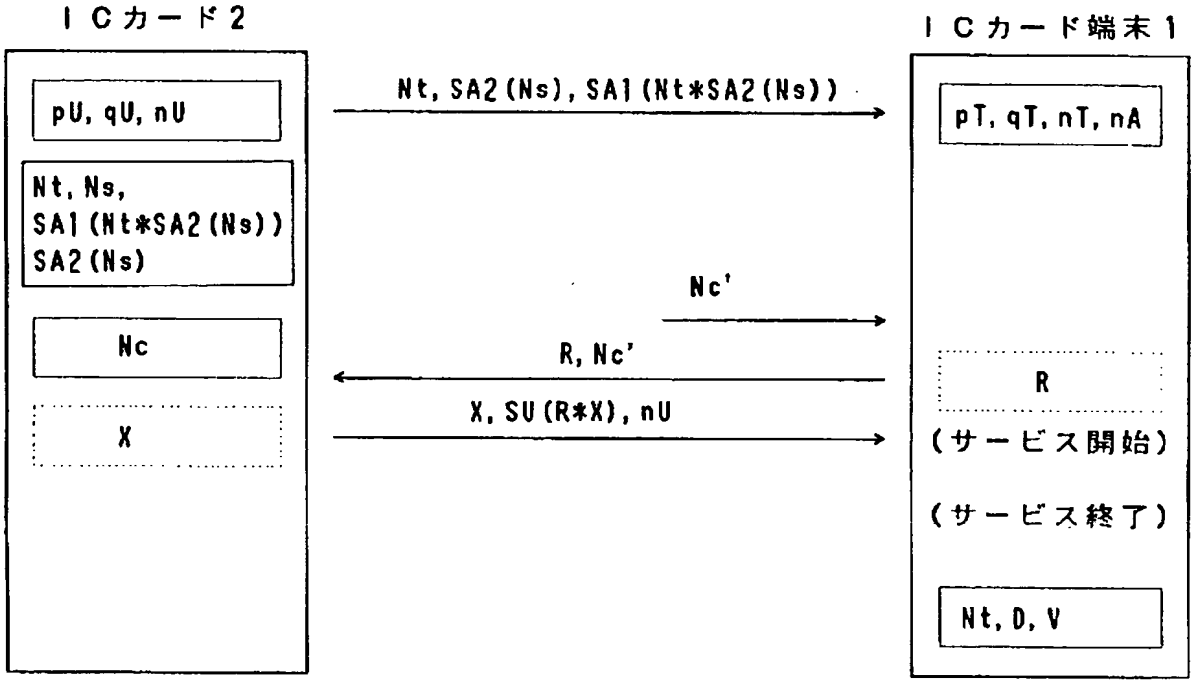
【図６】

図 6


ＩＣカード２
ＩＣカード端末１
pU, qU, nU
pT, qT, nT, nA
Nt, Ns,
SA1(Nt*SA2(Ns))
SA2(Ns)
R
X
Nc
Nt, SA2(Ns), SA1(Nt*SA2(Ns))
暗証番号登録
(暗証番号登録)
Nt'
Ns'
Ns'
(認証ＯＫ)
Nc
R
X, SU(R*X), nU
Nc, ST(R*X*Nc), nT

【図７】

図 7


ＩＣカード２
ＩＣカード端末１
pU, qU, nU
Nt, Ns,
SA1(Nt*SA2(Ns))
SA2(Ns)
Nc
X
Nt, SA2(Ns), SA1(Nt*SA2(Ns))
Nc'
R, Nc'
X, SU(R*X), nU
pT, qT, nT, nA
R
(サービス開始)
(サービス終了)
Nt, D, V

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.